UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/010,974	12/05/2001	Royce E. Slick	36.P327	9396

5514 7590 07/11/2006

FITZPATRICK CELLA HARPER & SCINTO
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER	
CERVETTI, DAVID GARCIA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 07/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/010,974	**Applicant(s)** SLICK ET AL.	
	Examiner David G. Cervetti	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 April 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5 and 7-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5 and 7-33* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 October 2005* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed April 28, 2006, have been fully considered but they are not persuasive.

2. Claims 1-5 and 7-33 are pending and have been examined. Claims 6 and 34 have been cancelled.

Response to Amendment

3. The objection to the drawings is withdrawn.

4. The remarks on paragraphs 6 through 10 of the previous Office Action are withdrawn.

5. The following prior art has been cited on this or a prior Office Action: **Currans** (US Patent 6,971,007), **Wiegley** (US Patent Number: 6,711,677), **Lohstroh** et al. (US Patent Number: 5,953,419, hereinafter Lohstroh), **Langford** et al. (US Patent Number: 6,470,450, hereinafter Langford), **Young** et al. (US Patent Number: 6,473,508, hereinafter Young), **Galasso** et al. (US Patent 6,148,387, hereinafter Galasso).

6. Applicant's arguments that Wiegley purposes for verifying the key are fully different from the instant application are not persuasive, since Wiegley still verifies the encryption key. Furthermore, Applicant's argument that the prior art of record does not teach or suggest verification in response to recognition of a printing instruction is not persuasive. Examiner submits that, first, it is inherent in Wiegley's to recognize the printing instruction (fig 3A-B), Wiegley does not expressly disclose that the verification occurs as a response to recognizing a printing instruction, but does teach "initiating a secure print session" and then, verification.

7. ***The applicant has not traversed the examiner's use of official notice with regards to the claimed limitations found in claims 2, 9, and 15, these features are taken by the examiner to be admitted prior art since the applicant has not adequately challenged the examiner's use of official notice (see MPEP 2144.03(c), 2144.04).***

Continued Examination Under 37 CFR 1.114

8. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

Claim Objections

9. Claim 12 is objected to because of the following informalities: "security algorithm", perhaps "encryption algorithm" was intended. Appropriate correction is required.

10. Claims 24-26 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The method is not further limited.

Claim Rejections - 35 USC § 112

11. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

12. Claims 1, 22-23, 27-28, and 31 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. See MPEP § 2172.01. The omitted structural cooṕerative relationships are: how/where are the method steps performed, computing device or target device, how are the two devices communicating?

Claim Rejections - 35 USC § 103

13. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

14. Claims 1-2, 5, 7-16, 19-21, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegley, and further in view of Menezes et al. (NPL "Handbook of Applied Cryptography", hereinafter Menezes).

Regarding claims 1 and 27, Wiegley teaches a method for securely storing a public key for encryption of data in a computing device, the method using a user-specific key pair which is securely stored in the computing device, the method comprising: a receiving step of receiving a target public key corresponding to a target device (column 4, lines 30-35);

- an obtaining step of obtaining a user-specific key pair from a secure registry (column 4, lines 47-65);

- a key encrypting step of using a user-specific private key from the user-specific key pair to create a target key verifier based on the target public key (column 4, lines 47-65);
- a storing step of storing the target key verifier and the target public key in a storage area (column 4, lines 47-65);
- a retrieving step of retrieving the target key verifier and the target public key from the storage area (column 5, lines 4-15);
- a recognizing step of recognizing a printing instruction (fig 3A-B, columns 3-4);
- a verification step of applying, in response to recognizing the printing instruction, a user-specific public key from the user-specific key pair to the target key verifier for verifying the authenticity of the target public key (column 4, lines 47-65).

Wiegley teaches a data-encrypting step of encrypting data (column 4, lines 57-60) using a session key, and encrypting the session key using the printer's public key (column 4, lines 52-55).

Wiegley does not expressly disclose a data encrypting step of encrypting data with the target public key, in the case that the authenticity of the target public key is verified, thereby creating encrypted data for transmission to the target device.

However, Menezes teaches using hash functions for data integrity in conjunction with digital signature schemes (pp. 321-323, 427-433). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the data using the printer's public key and provide a verifier for security purposes. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use a receiver's public key to encrypt a message destined to a receiver and to provide authentication, data integrity, and non-repudiation services by using digital signatures (Menezes, pages 425-428).

Regarding claim 2, the combination of Wiegley and Menezes does not expressly disclose wherein the user-specific key pair is obtained from a key function call which is supported by an operating system executing in the computing device. However, these features have been admitted per applicant to have been conventional and well known to digital rights management systems at the time the invention was made.

Regarding claim 5, the combination of Wiegley and Menezes teaches wherein the target key verifier created in the key encrypting step is an encrypted version of the target public key (Menezes, pp. 321-323, 427-433, Wiegley, column 4, lines 30-60).

Regarding claim 7, the combination of Wiegley and Menezes teaches wherein the verification step includes decrypting the target key verifier with the user-specific public key using a decryption algorithm (Wiegley, column 5, lines 4-24).

Regarding claim 8, the combination of Wiegley and Menezes teaches wherein the verification step further includes using a key verification algorithm to compare the decrypted target key verifier to the target public key for verifying the authenticity of the target public key (Wiegley, column 5, lines 4-24).

Regarding claim 10, the combination of Wiegley and Menezes teaches wherein the target key verifier created in the key encrypting step is a digital signature of the target public key (Menezes, pp. 321-323, 427-433).

Regarding claim 11, the combination of Wiegley and Menezes teaches wherein the digital signature of the target public key is created by applying a hashing algorithm to the target public key to obtain a target key hash, and then encrypting the target key hash with the user-specific private key using an encryption algorithm (Menezes, pp. 321-323, 427-433).

Regarding claim 12, the combination of Wiegley and Menezes teaches wherein the digital signature of the target public key is created by applying a hashing algorithm to the target public key to obtain a target key hash, and then subjecting the target key hash to a security algorithm (Menezes, pp. 321-323, 427-433).

Regarding claim 13, the combination of Wiegley and Menezes teaches wherein the verification step includes decrypting the target key verifier with the user-specific public key using a decryption algorithm to obtain a decrypted target key hash (Wiegley, column 6, lines 14-27, Menezes, pp. 321-323, 427-433).

Regarding claim 14, the combination of Wiegley and Menezes teaches wherein the verification step further includes reapplying a hashing algorithm to the target public key to obtain a new target key hash and using a hash verification algorithm to compare the decrypted target key hash to the new target key hash for verifying the authenticity of the target public key (Menezes, pp. 321-323, 427-433).

Regarding claims 9 and 15, the combination of Wiegley and Menezes does not expressly disclose wherein the verification step is performed by a verification function call which is supported by an operating system executing in the computing device. However, these features have been admitted per applicant to have been conventional and well known to digital rights management systems at the time the invention was made.

Regarding claim 16, the combination of Wiegley and Menezes teaches wherein the receiving step includes applying a hashing algorithm to the received target public key to obtain a received target key hash and using a hash verification algorithm to compare the received target key hash to a test target key hash for verifying the authenticity of the received target public key (Menezes, pp. 321-323, 427-433).

Regarding claim 19, the combination of Wiegley and Menezes teaches wherein the target device is a printer (Wiegley, column 4, lines 30-45). The combination of Wiegley and Menezes does not expressly disclose that the target public key is a printer public key. However, Wiegley does teach sending a session identifier and the printer public key to the device and Menezes teaches using hash functions for data integrity in conjunction with digital signature schemes (pp. 321-323, 427-433). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the printer public key instead of the session identifier. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use a receiver's public key to encrypt a message destined to said receiver.

Regarding claim 20, the combination of Wiegley and Menezes teaches wherein, in the receiving step, the printer public key is received in response to a key request sent to the printer (Wiegley, column 3, lines 62-67, column 4, lines 1-20).

Regarding claim 21, the combination of Wiegley and Menezes teaches wherein the method is performed in a printer driver executing on the computing device (Wiegley, column 3, lines 40-56).

15. Claims 3-4 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegley and Menezes, and further in view of Lohstroh.

Regarding claim 3, the combination of Wiegley and Menezes does not expressly disclose wherein the operating system securely maintains a user-specific key pair for each of a plurality of users of the computing device. However, Lohstroh et al. teach wherein the operating system securely maintains a user-specific key pair for each of a plurality of users of the computing device (column 23, lines 57-67, column 24, lines 1-11). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to have the operating system maintain a key-pair associated with each user. One of ordinary skill in the art would have been motivated to do so to further control access to secure data (Lohstroh et al., column 4, lines 1-15).

Regarding claim 4, the combination of Wiegley, Menezes, and Lohstroh teaches wherein each user-specific key pair can only be accessed by providing the operating system with user identification data corresponding to the user-specific key pair (Lohstroh , column 23, lines 57-67, column 24, lines 1-11).

Regarding claim 22, Wiegley teaches a method for securely storing a printer public key for encryption of print data in a computing device, the method using a user-specific key pair which is securely stored in the computing device, the method comprising: a receiving step of receiving a printer public key corresponding to a printer (column 4, lines 30-35);

- a first hashing step of applying a hashing algorithm to the printer public key to create a first printer key hash (column 5, lines 48-67, column 6, lines 1-50);
- an encryption step of applying an encryption algorithm to encrypt the first printer key hash with a user-specific private key from the user-specific key pair, thereby creating a printer key signature (column 5, lines 48-67, column 6, lines 1-50);
- a storing step of storing the printer key signature and the printer public key in a storage area (column 4, lines 47-65);
- a retrieving step of retrieving the printer key signature and the printer public key from the storage area (column 5, lines 4-15);
- a second hashing step of applying the hashing algorithm to the retrieved printer public key to create a second printer key hash (column 6, lines 14-27);
- a decrypting step of applying a decryption algorithm to decrypt the printer key signature with a user-specific public key from the user-specific key pair, thereby retrieving the first printer key hash (column 6, lines 14-27);
- a recognizing step of recognizing a printing instruction (fig 3A-B, columns 3-4);

- a verification step of applying, in response to recognizing the printing instruction, a verification algorithm to compare the first printer key hash with the second printer key hash, for verifying the authenticity of the retrieved printer public key (column 6, lines 14-27).

Wiegley teaches a data-encrypting step of encrypting data (column 4, lines 57-60) using a session key, and encrypting the session key using the printer's public key (column 4, lines 52-55).

Wiegley does not expressly disclose a print data encrypting step of applying an encryption algorithm to print data using the retrieved printer public key, in the case that the authenticity of the retrieved printer public key is verified, to create encrypted print data for transmission to the printer, ***nor*** an obtaining step of obtaining a user-specific key pair from a secure registry upon receipt of a corresponding user identification (column 4, lines 47-65).

However, Lohstroh teaches an obtaining step of obtaining a user-specific key pair from a secure registry upon receipt of a corresponding user identification (column 23, lines 57-67, column 24, lines 1-11) and Menezes teaches using hash functions for data integrity in conjunction with digital signature schemes (pp. 321-323, 427-433). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the data using the printer's public key and provide a verifier for security purposes. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use a receiver's public key to encrypt a message destined to a receiver and to provide authentication, data integrity, and non-repudiation services by using digital signatures (Menezes, pages 425-428).

16. Claims 17-18 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegley and Menezes, and further in view of Langford.

Regarding claim 17, the combination of Wiegley and Menezes does not expressly disclose wherein the test target key hash is input by a user. However, Langford teaches wherein the test target key hash is input by a user (column 7, lines 50-67, column 8, lines 1-20). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to compare a computed hash value of received data to a trusted hash value for verifying the authenticity of the received value. One of ordinary skill in the art would have been motivated to do so because it is well known in the art to verify authenticity of received data by using hash values (Langford, column 7, lines 60-67, column 8, lines 1-20).

Regarding claim 18, the combination of Wiegley, Menezes, and Langford teaches wherein the target device is a printer (Wiegley, column 4, lines 30-45) and wherein the test target key hash is obtained from a test page printed by the printer (Langford, column 7, lines 56-60).

Regarding claims 23, Wiegley teaches a method for authentication of a printer public key received by a computing device, the method comprising: a first receiving step of receiving in the computing device a printer public key corresponding to a printer (column 4, lines 30-35); a hashing step of applying a hashing algorithm to the printer public key to create a first printer key hash (column 5, lines 48-67, column 6, lines 1-50);

- a recognizing step of recognizing a printing instruction (fig 3A-B, columns 3-4);
- a verification step of applying, in response to recognizing the printing instruction, a verification algorithm to compare the first printer key hash with the second printer key hash, for verifying the authenticity of the received printer public key (column 6, lines 14-27); and
- a storing step of storing, in the case that the authenticity of the received printer public key is verified in the verification step, the received printer public key in a memory area of the computing device (column 4, lines 30-46).

Wiegley does not expressly disclose

- a second receiving step of receiving in the computing device a predetermined second printer key hash obtained from a test page printed by the printer, wherein the second printer key hash is input into the computing device by a user-input means connected to the computing device.

However, Menezes teaches using hash functions for data integrity in conjunction with digital signature schemes (pp. 321-323, 427-433) and Langford teaches a second receiving step of receiving in the computing device a predetermined second printer key hash obtained from a test page printed by the printer, wherein the second printer key hash is input into the computing device by a user-input means connected to the computing device (column 7, lines 50-67, column 8, lines 1-20).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to compare a computed hash value of received data to a trusted hash value for verifying the authenticity of the received value. One of ordinary skill in the art would have been motivated to do so because it is well known in the art to verify authenticity of received data by using hash values (Langford et al., column 7, lines 60-67, column 8, lines 1-20) and to use a receiver's public key to encrypt a message destined to a receiver and to provide authentication, data integrity, and non-repudiation services by using digital signatures (Menezes, pages 425-428).

17. Claims 28, 30, 31, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegley and Menezes, and further in view of Young.

Regarding claims 28 and 31, Wiegley teaches transferring encrypted print data to a printer, comprising: retrieving means/step for receiving a public key from said printer (column 3, lines 62-67, column 4, lines 30-35);

- generating means/step for generating verification information from the public key (column 5, lines 48-67, column 6, lines 1-50);
- recognizing means/step for recognizing a printing instruction (column 2, lines 40-56, fig 3A-B, columns 3-4).

Wiegley does not expressly disclose

- verification means/step for verifying, in response to the recognition of the printing instruction, that the public key is not changed from the retrieved public key; and
- control means/step for controlling encryption processing which is performed by using said public key when the retrieved public key is verified as

unchanged, and which is not performed when the retrieved public key is verified as changed.

However, Young teaches verification means for verifying, in response to the recognition of the printing instruction, that the public key is not changed from the retrieved public key (column 9, lines 22-36); and control means for controlling encryption processing which is performed by using said public key when the retrieved public key is verified as unchanged, and which is not performed when the retrieved public key is verified as changed (column 9, lines 22-36) and Menezes teaches using hash functions for data integrity in conjunction with digital signature schemes (pp. 321-323, 427-433). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the data using the printer's public key and provide a verifier for security purposes and to verify the public key of a sender at a receiving end (the printer sending its public key to the information apparatus) and based on this verification process, proceed accordingly (encrypt data and send it to the printer). One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use a receiver's public key to encrypt a message destined to a receiver and to provide authentication, data integrity, and non-repudiation services by using digital signatures (Menezes, pages 425-428) and to verify the authenticity of a received message (Young, column 9, lines 32-36).

Regarding claims 30 and 33, the combination of Wiegley, Menezes, and Young teaches wherein said control means controls the encryption processing to encrypt the print data by using a user specific key obtained by an obtaining means and to encrypt the user specific key by using the public key (Young, column 9, lines 22-36).

18. Claims 29 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegley, Menezes, and Young, and further in view of Langford.

Regarding claims 29 and 32, the combination of Wiegley, Menezes, and Young does not expressly disclose obtaining means for obtaining a user specific key stored in a computer; input means for inputting authentication information; and determining means for determining whether to allow the obtaining means to obtain the user specific key. However, Langford teaches obtaining means for obtaining a user specific key stored in a computer (column 5, lines 56-67, column 6, lines 1-29); input means for inputting authentication information (column 5, lines 56-67, column 6, lines 1-29); and determining means for determining whether to allow the obtaining means to obtain the user specific key (column 5, lines 56-67, column 6, lines 1-29). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate user access to a user specific key. One of ordinary skill in the art would have been motivated to do so to protect user information (Langford, column 1, lines 35-65).

19. Claims 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegley and Menezes, and further in view of Lohstroh and Langford.

Regarding claims 24-26, the combination of Wiegley, Menezes, Lohstroh, and Langford teaches:

- a program memory for storing process steps executable to perform a method according to any of Claims 1 to 23; and a processor for executing the process steps stored in said program memory (Wiegley, column 4, lines 1-67),
- Computer-executable process steps stored on a computer readable medium, said computer-executable process steps for authenticating a public key for encryption of data, said computer-executable process steps comprising process steps executable to perform a method according to any of Claims 1 to 23 (Wiegley, column 4, lines 1-67), and
- computer-executable process steps to authenticate a public key for encryption of data, said computer-executable process steps comprising process steps executable to perform a method according to any of Claims 1 to 23 (Wiegley, column 4, lines 1-67).

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Lee (US Patent 6,628,413) teaches a JAVA printer using any available security technique (columns 3-6). Lloyd (US Patent Application Publication 2003/0014640) teaches a printer using public key encryption and hash functions to verify information in transit has not been tampered with (paragraphs 20-30). Wu et al. (US Patent Application Publication 2002/0042884) teaches a printer, digital certificate, hash functions, and public key encryption for providing a secure printing environment, authenticating a printer, etc. (pages 7-13). Takaragi et al. (US Patent 6,370,247) teaches using hash values and encryption for data protection (columns 5-6). Fischer

(US Patent 5,005,200) teaches a public key/digital signature system. Debry (US Patent 6,918,042) teaches a printer storing a key and a certificate authority also storing said key.

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

22. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

23. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DGC